DOCUMENT RESUME

ED 202 438 HE 013 973

TITLE	Report of the Public Cryptography Study Group.
INSTITUTION	American Council on Education, Washington, D.C.
SPONS AGENCY	National Science Foundation, Washington, D.C.
REPORT NO	NSF-CDP-8006675
PUB DATE	7 Feb 81
NOTE	24p.
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Academic Freedom; Advisory Committees; Censorship; Civil Liberties; *Confidentiality; Constitutional Law; Federal Government; Foreign Countries; *Government Role; Higher Education; *Information Dissemination; Information Networks; Information Utilization; International Relations; Legal Problems; Position Papers; *Publications; Research Reports; *Research Utilization; Technological Advancement; Telecommunications
IDENTIFIERS	*Cryptography; *National Security Agency

ABSTRACT

Concerns of the National Security Agency (NSA) that information contained in some articles about cryptography in learned and professional journals and in monographs might be inimical to the national security are addressed. The Public Cryptography Study Group, with one dissenting opinion, recommends that a voluntary system of prior review of cryptology manuscripts be instituted on an experimental basis. Cryptography is the body of knowledge that deals with methods of information protection. NSA is concerned that research and dissemination in this field could lead to the publication of cryptographic principles or applications similar to those used by the United States Government. NSA claims that this work may enable foreign powers to engage more successfully in cryptanalytic attacks upon the secure telecommunications of our government and that papers dealing with weaknesses in cryptosystems may be used by other governments and prompt them to adopt more sophisticated and less vulnerable systems. Although the study group views any system of prior review involving governmental agencies as a possible disincentive to academics and others to undertake research, guidelines are suggested for a proposed voluntary system. The dissenting study group opinion to the voluntary system is also presented. In "The Case Against Restraints on Non-Governmental Research in Cryptography," George I. Davida argues that the national security interests of the country are broader than the narrow mission of the NSA, which is data-gathering; that restraints would adversely affect that quality and direction of basic research in computer science, engineering, and mathematics; that restraints would be unconstitutional and would lead to legal entanglements and international complications, and that restraints would be ineffective in achieving the NSA's objectives. (SW)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED202438

REPORT OF THE PUBLIC CRYPTOGRAPHY STUDY GROUP

Prepared for

American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Todd Furnish

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

IHE013 923

REPORT OF THE PUBLIC CRYPTOGRAPHY STUDY GROUP

Prepared for

American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

FOREWORD

This report has been prepared by the members of the Public Cryptography Study Group.[1] The Study Group was assembled by the American Council on Education (ACE) in response to a request by the National Security Agency; that agency has indicated concern that information contained in some articles in learned and professional journals and in monographs might be inimical to the national security. The Study Group held its first meeting on March 31, 1980, and transacted its business in a series of meetings through February 1981.(The membership of the Study Group is listed on page 2.)

The Study Group has recommended that a voluntary system of prior review of cryptology manuscripts be instituted on an experimental basis. While the group would prefer no such system of review, its members, with one dissent, accepted as a working premise NSA's concern that some information contained in cryptology manuscripts could be inimical to the national security of the United States and see the proposed system as a potential way to test that working premise. The group rejected a compulsory statutory solution to the perceived problem.

In assembling the Study Group, ACE sought recommendations of individuals who might participate from several professional societies and organizations. The American Association of University Professors (AAUP), the American Mathematical Society (AMS) the Association for Computing Machinery (ACM), the Computer Society of the IEEE (IEEE/CS), the Institute of Electrical and Electronics Engineers (IEEE), and the Society for Industrial and Applied Mathematics (SIAM) made such recommendations. Although nominated by professional societies, the members served as individuals on behalf of ACE and the final report is a product of the American Council on Education.

The Study Group hopes that the recommended voluntary system will prove effective. Success, however, is dependent upon the endorsement and good faith cooperation of NSA on one side and authors, researchers, professional societies, and publishers on the other. Therefore, it is the intent of the Study Group that this report be transmitted to all relevant professional societies, as well as receiving widespread public distribution. The Study Group also recommends that a timely review be conducted concerning the operations of the recommended voluntary system, should one emerge, and that the relevant professional societies receive and record comments on such operations for use in the future review.

[1]This material is based upon work supported by the National Science Foundation under Grant No. CDP-8006675. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

MEMBERSHIP

Dean Werner A. Baum — CO-CHAIRMAN
College of Arts and Sciences
(and Chancellor Emeritus, U. of Wisconsin - Milwaukee)
The Florida State University
Tallahassee, FL 32306

David H. Brandin
Vice President
Computer Science and Technology Division
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025
(Nominated by the Association for Computing Machinery)

Professor R. Creighton Buck
Department of Mathematics
Van Vleck Hall
University of Wisconsin
Madison, WI 53706
(Nominated by the American Mathematical Society)

Professor George I. Davida
Department of Electrical Engineering and Computer Science
University of Wisconsin - Milwaukee
Milwaukee, WI 53201
(Nominated by the Computer Society of IEEE)

Professor George Handelman
Department of Mathematical Sciences
Rensselaer Polytechnic Institute
Troy, NY 12181
(Nominated by the Society for Industrial and Applied Mathematics)

Professor Martin E. Hellman
Department of Electrical Engineering
Stanford University, Durand 135
Stanford, CA 94305
(Nominated by the Institute of Electrical and Electronics Engineers)

Chancellor Ira Michael Heyman – CO-CHAIRMAN
Chancellor's Office, 200 California Hall
University of California, Berkeley
Berkeley, CA 94720

Professor Wilfred Kaplan
Department of Mathematics
The University of Michigan
347 West Engineering Building
Ann Arbor, MI 48109
(Nominated by the American Association of University Professors)

Daniel C. Schwartz
General Counsel
National Security Agency
Central Security Service
Fort George G. Meade, MD 20755

1. INTRODUCTION

Two years ago, Vice-Admiral B. R. Inman, Director of the National Security Agency, publicly indicated his deep concern that some information contained in published articles and monographs on cryptography[2] endangered the mission of NSA and thus the national security. Existing statutes do not regulate the domestic publication of unclassified information relating to cryptography.[3] Admiral Inman proposed a dialogue with the academic community on how to reconcile the national needs with the tradition that scholarly publication should be free from restriction.

In reponse to Admiral Inman's initiative, the American Council on Education proposed establishment of a Public Cryptography Study Group, bringing together representatives of the academic world and of NSA. The National Science Foundation agreed to provide funding to the ACE for this purpose. This report is the product of the Group's efforts over a year.

In addition to the dilemma of reconciling important First Amendment rights with NSA's concern for the protection of the nation's communications security and intelligence-gathering capabilities, the group soon recognized that it was essential to take into account the emerging uses of cryptography in the public sector.

In an era of instantaneous communication and pervasive computer data bases, it is becoming increasingly important to protect the privacy of both individuals and corporations, often using the tools previously used only by national governments.

There is growing evidence that enhanced security for unclassified but sensitive information will be needed in a wide variety of applications, ranging from personal records (insurance, criminal, health, law enforcement) to commercial proprietary and financial data in storage or in

---

[2]Cryptography is the body of knowledge that deals with methods of information protection. Methods that transform text, using a key, so that it becomes unintelligible and therefore useless to those not meant to have access to it, are called *encryption* methods. Transforming the encrypted information back to its original form is called *decryption*.

[3]Provisions of the United States Criminal Code and related regulations make it a crime to receive, disclose, communicate , or publish various kinds of documents and information. Section 798 of Title 18 specifically prohibits knowing communication, transmission, or publication of any *classified* information pertaining to any "code, cipher or cryptographic system," or any "communication intelligence activity" of the United States or any foreign govermnment to an unauthorized person. It also prohibits the use of such classified information in a manner prejudicial to the interests of the United States or to the benefit of any foreign government. Section 793 of Title 18 prohibits the obtaining or delivering of information relating to the national defense with knowledge that the information is to be used or could be used to the injury of the United States or the advantage of any foreign nation, or revealing national defense information through gross negligence where the information was initially in the individual's lawful possession. In addition, 18 U.S.C. Section 952 prohibits dissemination of information about diplomatic codes. A related statute, 50 U.S.C. Section 403(d), charges the Director of Central Intelligence with the responsibility to protect intelligence sources and methods pursuant to which he has promulgated intelligence directives binding only on the government.

transit electronically. As the major world economies continue the trend toward information dependence, e.g., electronic mail, electronic funds transfer, point of sale terminals, etc., protection of business and even home computer systems from unauthorized monitoring or tampering will become increasingly important.

In many of these areas, cryptography is one of the most effective ways for providing the requisite security. Restriction of public research and development in cryptography might have an adverse effect on the ability of American industry to compete in world telecommunications and data-processing markets.

2. THE NATIONAL SECURITY CONCERNS

Traditionally, national security information has been of a diplomatic or military nature. However, as the nation moves to an information-based economy, protecting valuable or sensitive commercial and personal information becomes a concern of national security in a broader sense. Inadequate security for such data could have profound effects on the nation.

The Study Group recognizes that increased research activity in cryptology by persons and institutions in the nongovernmental arena may result in advances in the development of cryptographic systems. Work directly in cryptology or in related fields may have a beneficial impact on developments in computer science, electrical engineering, and mathematics which have potential benefits to fields apart from cryptology. Products developed in the course of this research may be very useful in providing effective telecommunications for nongovernmental and governmental purposes. Although governmental efforts in cryptology have traditionally led private efforts, these private efforts may develop new techniques or insights that could benefit broader government interests. The Study Group also recognizes that significant nongovernmental research in this area may be applied over the long run to increase communication protection in commercial and private fields, thus enhancing the security of private and commercial communications and ultimately furthering the nation's welfare and security in a broader sense.

Some researchers in the public sector have expressed serious concern about the fragility of our developing information-based society. It has been suggested, for example, that a foreign power might inject misleading data into the statistics used for computing the nation's money supply, causing the government to take dangerously inappropriate action.

At the same time, however, concerns have been expressed by the National Security Agency that extensive private work in cryptology and related fields may significantly and directly adversely affect the security of the nation's sensitive official communications and the nation's ability to obtain and understand foreign intelligence. NSA claims that the risks become greater to the extent that work moves away from pure research and into the application of theoretical developments to specific problems of communication protection and the development of actual protection systems.

One of the areas of concern by the NSA is that substantial work in cryptographic and cryptanalytic techniques together with a widespread dissemination of resulting discoveries could lead to the publication of cryptographic principles or applications similar to those used by the United States Government. NSA claims that this work may enable foreign powers to engage more successfully in cryptanalytic attacks upon the secure telecommunications of our government. Another area of concern to the NSA is that papers dealing with weaknesses in

cryptosystems that may be used by other governments may alert these governments to the weaknesses of their own systems and thus prompt them to adopt more sophisticated and less vulnerable systems. In this manner, the United States may be denied needed intelligence.

The National Security Agency has expressed interest in considering what type of procedure could be developed that would provide a systematic means by which publications relating to cryptology could be reviewed to determine whether such publications would have an overriding adverse impact on the national security as it pertains to NSA's mission. There exist a number of federal statutes and regulations that govern the dissemination of information that is classified or controlled by the U.S. Government on the basis of national security or foreign policy concerns. It is felt by NSA, however, that these statutes and regulations do not cover publication of articles or the dissemination of general research information within the United States. They also may not cover such publication abroad unless such information is otherwise classified by the government or its export is controlled for national defense or foreign policy reasons.

Existing statutes do not regulate the domestic publication of unclassified information relating to cryptology. Restrictions on foreign dissemination of certain information relating to cryptology are contained in the provisions of the Arms Export Control Act (22 U.S.C. 2778), which authorizes the President to compile a United States Munitions List and to issue the International Traffic and Arms Regulation (ITAR) (22 CFR 21), which identifies specific types of articles, the export of which is subject to the granting of a license by the Secretary of State. Cryptographic equipment is explicitly designated as a category subject to such export control. Category XVIII of the ITAR includes technical information relating to articles on the Munitions List. This latter provision has been subject to some question by the Office of Legal Counsel in the Department of Justice as being overly broad.

Munitions Control Letter No. 80, February 1980, issued by the Department of State provided further clarification under ITAR with respect to cryptology by making clear that the export restrictions do not prescribe prepublication review for publication in the United States of any publications including "general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment" otherwise covered by the export licensing restrictions.

There has been some disagreeement within the government concerning the extent of the need to control technical data. The Department of Commerce, in the context of a review of the Export Administration Act, has indicated that its assessment is that the availability of technical data that are of significance to U.S. national security and foreign policy interests is likely to be minor. On the other hand, the Departments of Defense and State, in the context of the Arms Export Control Act under which the ITAR is promulgated, have continued to emphasize the need to effectively control technical data. In addition, studies conducted for the Department of Defense led to the establishment within the Export Administration Act of the

Military Critical Technologies List, which is heavily focused on knowledge related to design, manufacturing, application, operation, and maintenance of such critical technologies. Cryptographic items are not processed under the Export Administration Act of 1979 unless there is a prior determination by the Department of State that jurisdiction over a specific item should be transferred to Commerce for processing under that Act.

Finally, Section 181 of Title 35 U.S.C. permits the imposition of a secrecy order upon a patent application when issuance of a public patent would be detrimental to the national security. The statute also provides for compensation for the nongovernment inventor financially injured as a result of a secrecy order. There is no provision in the law pertaining to patent secrecy orders that applies directly to publication or to any requirement for prepublication review. Additionally, a patent secrecy order for a patent application based on published material is not possible.

While there is currently no formal procedure or requirement for prepublication review by NSA of publications relating to cryptology, some authors and publishers routinely and voluntarily submit proposed publications to NSA for review and comment as to the sensitivity of the information involved. NSA currently has no statutory authority to require submission of proposed publications for the purpose of review or to require changes in publications prepared outside the agency and not under NSA contract or grant. The National Science Foundation has announced, however, that, while it does not currently have classification authority, it has responsibility under routine executive orders to refer information developed in NSF-supported cryptologic research it believes may be classifiable to NSA for possible classification.[4] NSF indicates, however, that it makes no essential difference, from the standpoint of classification, whether research is supported by NSA or NSF.

---

[4]The following text, included for completeness, is the standard NSF Grant Instrument Clause for Potentially Classifiable Research.

The National Science Foundation does not expect that results of basic research it supports will be classified, except in very rare instances. Further, while NSF does not have classification authority, it has the responsibility to refer any information that NSF has reason to believe might require classification to the agency with appropriate subject matter interest and original classification authority.

Therefore, the grantee is responsible for immediately notifying the NSF Program Official, of any data, information, or materials developed under this grant which may require classification. The grantee shall, prior to dissemination or publication of potentially classifiable research results obtained under this grant, allow NSF the option to review such materials. The grantee shall defer dissemination or publication pending the review and determination that the results are not classified, provided such review and determination are completed within sixty days of receipt by NSF of such material. If the review results in classification, the grantee agrees to cooperate with NSF or other U.S. agencies in securing all related notes and papers. Policies relating to this subject are set forth in the NSF *Grants Policy Manual* Section 794, "National Security."

3. DELIBERATIONS AND CONCLUSIONS

As a starting point for its work, Admiral Inman proposed that the Study Group consider the acceptability of restrictions on domestic dissemination of nongovernmental technical information relating to cryptology. He proposed several criteria that should be taken into account for both policy and legal reasons:

(1) The restrictions should apply only to a central core of critical cryptologic information that is likely to have a discernible adverse impact on the national security.

(2) Law and regulations should make these criteria as clear as is possible without revealing information damaging to the national security.

(3) The burden of proof in imposing any restriction on dissemination should be borne by the government.

(4) There should be judicial review of any such government action, perhaps by a specially constituted court that could act under suitable security precautions, and the government should bear the burden of obtaining judicial approval of its action.

(5) There should be full, fair, and prompt compensation for any company or person losing the economic benefit of information by virtue of governmentally imposed restrictions on dissemination.

Admiral Inman's criteria would suggest a statute that would create a system of restrictions. There are basically two ways to proceed by statute. One is to make it a crime to disseminate defined cryptologic information. Under such a system, NSA (or another agency) would monitor published information and would recommend criminal prosecution in instances where defined cryptologic information had been published. The other means is by required prepublication review. The statute would make it mandatory to obtain clearance from a designated agency, such as NSA, before publishing defined cryptologic information. Publishing without obtaining clearance would be a criminal act. The impact of the latter system could be moderated, as suggested by Admiral Inman, by requiring a judicial order confirming the agency's decision to restrict dissemination and by payment of compensation where permission is denied. Still, however, it would be a crime to publish without seeking clearance or in contempt of the judicial restraining order.

Admiral Inman's criteria suggest a system of prepublication review. Such a system clearly would best serve Admiral Inman's concern by assuring the government's ability to preclude publication or dissemination of defined information. At the same time, however, such a system raises serious legal, policy, and practical questions.

Problems Associated with a Nonvoluntary System

The legal and political system of the United States, as expressed in the First Amendment to the Constitution, is generally opposed to both pre- and postpublication restraints. Although such opposition, historically, has been strongest where restraints have been placed on utterances related to political or social thought, the First Amendment applies to practically all speech, regardless of its description, with the possible exception of obscenity.[5] (For instance, the present Supreme Court has applied First Amendment protections to "commercial" speech, which previously had been treated as outside the ambit of the First Amendment.[6] Further, courts, as in the recent *Progressive Case*,[7] have assumed without debate that information of a technological or scientific nature is subject to First Amendment protections. It is clear that monographs and articles in professional journals and elsewhere concerning cryptography are within the ambit of this protection. As one legal scholar has observed, freedom of expression has historically related to four traditional and interrelated values:[8]

(1) individual self-fulfillment,

(2) the advance of knowledge and the discovery of truth,

(3) participation in decision making by all members of society, and

(4) maintenance of the proper balance between stability and change.

Writings on cryptology are closely related to (1) and (2), if not also to (3) and (4).

That speech falls within the protection of the First Amendment, however, does not mean that it cannot be regulated. In most recent instances, the Supreme Court has sought to balance the importance of the speech involved against the state interest sought to be protected by its regulation. In many cases, the Court has weighted the balance heavily in favor of free speech (a "preferred freedom") and subjected the opposing interests to "exacting scrutiny."[9] In others, it has been neutral or has weighted the balancing to the contrary.[10] It is difficult to discern a consistent theory with predictable results.

---

[5]*Roth v. United States* 354 U.S. 476, 1957. Even though determined to be outside the bounds of the First Amendment, because it is so removed from the "advancement of truth, science, morality, and arts in general... and its lack of redeeming social importance," the Court has carefully and consistently delineated narrow standards for permissible restraints on obscenity. Four dissenters to obscenity controls (Brennan, Stewart, Marshall and Stevens) are of the view that any such controls, at least for adults, are unconstitutional.

[6]*Bigelow v. Virginia*, 421 U.S. 809 (1975). See Emerson, *First Amendment Doctrine and the Burger Court*, 68 CAL. L. REV. 422, 458-61 (1980) (hereafter "Emerson").

[7]*United States v. Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis.), *request for writ of mandamus, den. sub. nom.* Morland v. Sprecher, 99 S. Ct. 3086, case dismissed, Nos. 79-1428, 79-1664 (7th Cir. Oct 1, 1979).

[8]Emerson 423

[9]Emerson 449

[10]Emerson 450-51

It is likely that the Court would balance in a neutral manner where the justification, adequately demonstrated, was that publication constituted a threat to national security.[11] The government, of course, would bear the initial burden of showing that such publication posed a significant threat.[12] Once this was shown to the Court's satisfaction, the issue properly would be whether the threat to security by the publication of a writing concerning cryptology outweighed the value of the writing itself, the maintenance of nongovernmental research programs in cryptology, unfettered academic and scientific inquiry, and similar threatened social values. Such a test, of course, could not come about without passage of legislation barring publication of privately generated information concerning cryptology. The legislative balancing implicit in its passage undoubtedly would be given some weight by the Court. Of considerable importance would be whether or not the legislation narrowly defined the regulated information. The legislation would more easily pass judicial scrutiny if a narrow and unambiguous definition was formulated because its chilling impact on cryptologic research would be minimized.

Historically, the *means* of regulating expression has been of central importance to constitutional validity. Although some regulation or restraint may be justified, the Court usually has required that the least drastic means be used. Punishment for uttering or otherwise publishing proscribed speech has been difficult to maintain; imposing a licensing system — or prior restraint — has been much more difficult. "The doctrine forbidding prior restraint is one of the major underpinnings of the system of freedom of expression. Its roots go back to the English censorship laws against which John Milton protested."[13]

There have been exceptions, however, to prohibitions on systems of prior restraint. One seminal case stated that the publication of "the number and location of troops" could be restrained.[14] The trial court in the *Progressive Case*[15] enjoined the publication of materials concerning the design and operations of nuclear weapons. The Supreme Court in another case[16] permitted a censorship board to screen out "obscene" films. Moreover, the present Supreme Court "does not [appear to] view the prior restraint doctrine as a prohibition on all prior restraints subject to certain categorical exceptions such as obscene motion pictures or communications about tactical military operations. Rather, in its view, the doctrine simply creates a

---

[11]Goldberg, *The Constitutional Status of American Science*, 1979 UNIV. of ILL. L. FORUM 1, 14-15 (1979)

[12]*New York Times Co. v. United States*, 403. U.S. 713 (1971)

[13]Emerson 454

[14]*Near v. Minnesota ex rel* Olson, 283 U.S. 697 (1931)

[15]Note 7, *supra.*

[16]*Times Film Corp. v. City of Chicago*, 305 U.S. 43 (1961)

'presumption' against the validity of the restraint and thereby imposes a 'heavy burden' on the government to justify the particular restriction then before the Court."[17] This is buttressed by the Court's action in the *Pentagon Papers Case*.[18] Three justices (Burger, Harlan, and Blackmun) would have upheld the injunction, believing that the courts should exercise only an extremely limited review where the executive has determined that the disclosure "would irreparably impair the national security." Thus they did not even require the satisfaction of a "heavy burden." Two others (Stewart and White), while recognizing the "concededly extraordinary protection against prior restraints," nevertheless were willing to allow an injunction upon a showing of "direct, immediate and irreparable damage to our nation or its people."

This Committee's Assessment

As stated, Admiral Inman's criteria suggested, for discussion, legislation which would set up a system of prior review of articles and monographs relating to cryptology. This Committee was formed by ACE to carry out such a discussion. Under Admiral Inman's criteria, such a system would be less objectionable than classic systems of prior restraint that vest in an administrator the legal authority to review proposed publications under discretionary standards and make it a crime to publish them without the administrator's approval. First, Admiral Inman proposed that the criteria for what is proscribed (i.e., what can be "censored") should be narrow. Secondly, NSA's General Counsel proposed as a departure point for discussion that the staff's decision be reviewable by a Board, including cleared persons from outside NSA, with a final decision by the Director. Thirdly, no suppression order could be effective unless ratified by a court after a judicial proceeding. Fourthly, the government would have the burden of proof in such a judicial proceeding. Finally, compensation would be paid to an author whose work was suppressed.

This Group feels that NSA's initiative in commencing a public dialogue is commendable and that the Agency has sought to craft a narrow and constructive solution to a problem that it perceives. We reject, however, the statutory solution that has been proposed for a number of reasons:

(1) We have not been in a position to assess the seriousness of the threat to the national security posed by the publication of selected articles and monographs on cryptology. Such an assessment would require security clearance of committee members and a deep understanding of cryptographic systems. We were offered such clearance, but this committee, made up of persons heavily involved with other tasks and without staff, was in no position to take on such a heavy work burden. Relatedly, we have no sophisticated idea of the types of information that NSA would seek to suppress — we thus cannot discern the reach of a system of prior restraint or adequately evaluate its justification.

---

[17]Emerson 457

[18]Note 11, *supra*.

(2) We have been in no position to gauge systematically the impact of a statutory prepublication review system on nongovernment research in cryptology or the economic or social losses that a negative impact might entail. Possible negative impacts include loss of scientific advancements and innovations which might lead to better security against invasions of privacy of individuals and commercial entities and enhanced opportunities for foreign trade. It is clear to us that cryptology has become important outside of government as electronic storage and transmission of data enlarge in the private sector.

(3) We have been unable to fashion a narrow and precise definition of that cryptologic information that should be kept secret. We feel that such a definition is essential to provide adequate notice in order to protect persons from criminal punishment for unintentional violation, to limit the discretion of regulators, and to lessen the inhibiting impact or chilling effect that would attend ambiguous or overbroad standards.

(4) We are impressed that, without the foregoing definition, a system that punishes publication of scientific and technological information, or subjects proposed publications to legally required prepublication review, is contrary to the values expressed in the legal and political history of the First Amendment.

(5) From a practical standpoint, any system of prior review will work best with the cooperation of the cryptology community. It seems clear that a voluntary system is likely to generate more cooperation than would a compulsory statutory system.

A Suggested Voluntary Procedure

The committee accepted as a working premise Admiral Inman's concern that some information contained in some articles and monographs could be inimical to the national security. In light of the preceding legal, policy, and practical analyses, we cannot recommend a statutory system of pre- or postpublication review. Under these circumstances, we recommend an alternative nonstatutory system designed to test on an ongoing basis Admiral Inman's hypothesis, which depends for its success on the voluntary cooperation of those whom NSA might seek to regulate. What follows is an outline of such a system that includes an Advisory Committee cleared to a level that enables it to test adequately our working premise on an on-going basis. The implementation of this system will require that NSA convince authors and publishers of its necessity, wisdom and reasonableness. We believe that NSA will be able to be convincing if it establishes a record in its dialogues and its administration that evidences sensitivity, narrow application and remedies, and a sense of restraint and reasonableness to those who are asked to cooperate. We believe that many researchers would welcome an opportunity to find out in advance whether what they plan to publish would directly and substantially risk compromising national security interests.

We realize that any system of prior review involving governmental agencies, even a voluntary one, creates an environment that might dampen the desire of academics and others to undertake research. In view of Admiral Inman's serious representations of threats to

national security, however, we recommend the system here outlined be tried on an experimental basis.

The Study Group also recommends that a timely review be conducted concerning the operations of the recommended voluntary system, should one emerge, and that the relevant professional societies receive and record comments on such operations for use in the future review.

Our recommendation of a voluntary procedure on a trial basis should not, however, be construed as endorsing any legislation that might be modeled on the proposed procedures.

The following guidelines are suggested for the proposed voluntary system:

(1) NSA would notify the cryptologic community, including authors and publishers, of its desire to review manuscripts concerning aspects of cryptology prior to publication.

(2) NSA, in consultation with appropriate technical societies, would define as precisely as possible those aspects of cryptology to be covered by the procedure.[19]

(3) NSA would invite authors to send manuscripts to NSA for review prior to publication.

(4) NSA would assure prompt review by its staff of submitted manuscripts and prompt response to authors with an explanation, to the extent feasible, of proposed changes, deletions, or delays in publication, if any.

(5) NSA would provide, in the case of unresolved disagreements, the opportunity for authors to obtain prompt review by an Advisory Committee of five persons (two appointed by the Director of NSA and three appointed by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Science), which would make a recommendation to the Director of NSA and to the author concerning the matters in issue. Members of the Advisory Committee shall have adequate clearance so that the committee can make informed recommendations.

(6) There would be a clear understanding that submission to the process is voluntary and neither authors nor publishers will be required to comply with suggestions or restrictions urged by NSA.

---

[19]There are two problems of definition: (1) stating criteria to identify those articles and monographs which NSA wishes to review; (2) stating criteria to be used by NSA and the Advisory Committee to determine information the disclosure of which would directly and substantially compromise national security interests. Criteria for the first task must be broader than for the second. Nevertheless, care should be taken in both instances to narrow the scope of application to the extent feasible, and both sets of criteria should be published to the greatest extent possible.

The Committee determined to leave the ultimate definitions to NSA in consultation with appropriate technical societies. It believes, however, that NSA at the outset should exclude from review or proscription information concerning, for example, general mathematics, engineering, computer science or statistics, and basic theoretical research.

THE CASE AGAINST RESTRAINTS ON NON-GOVERNMENTAL RESEARCH IN CRYPTOGRAPHY

George I. Davida

A minority report of the Public Cryptography Study Group
of the American Council on Education

INTRODUCTION

The objectives of this report are to present arguments against restraints on non-governmental cryptographic research. Time and space limitations preclude a complete treatment of the subject of cryptology and the history of the conflict between the National Security Agency and the academic researchers in cryptology. The report of the PCSG contains some of this material.

NSA OBJECTIONS

It is difficult to state precisely NSA's objections to the open publication of research papers pertaining to cryptology and allied areas. In general the NSA claims that its mission will be harmed by such publications. Specifically the NSA claims that

A. Foreign governments might use the cryptographic results to deny the NSA the ability to perform intelligence gathering.

B. The basic or applied research results might accidently lead to compromise of NSA designed cryptosystems.

In the rest of the report the area of cryptology will be discussed briefly and the validity of the NSA's claims will be examined.

CRYPTOLOGY AND ITS IMPORTANCE

While a complete treatment of this subject is not possible in this report, it is important to briefly examine the area and, to put it in proper context, the role it plays in Information Protection (or Data Security).

CRYPTOGRAPHY consists of methods for transforming data, using a key, to render the data unintelligible to someone not authorized to have it. The process of so transforming data is called ENCRYPTION. A legitimate user can transform the garbled data back to its original form, using a key. This process is called DECRYPTION. PLAINTEXT is encrypted into CIPHERTEXT.

CRYPTANALYSIS consists of methods that are used to transform encrypted data back to its original form without the knowledge of the key.

Information Protection (or Data Security) pertains to the protection of data processed by, stored in or transmitted by computers. To protect data, a large number of problems must be solved. We shall examine a few of them.

PHYSICAL SECURITY

Obviously the best security methods are worthless if someone could just walk off with data on tapes or disks. Thus the facilities housing the computer system must have controlled access that is effective. These problems are not peculiar to computer security and will not be discussed any further other than to point out that the increasing use of electronic locks involves encryption.

DATABASE SECURITY

This is an area of great concern to the researchers and the public. Martin Hellman, who was the first to express concern about the safety margin of commercial cryptosystems, has said that the United States is the most computerized country in the world and the one to lose the most from insufficiently secure systems.

The increase in the computerization of the society has led to the construction of a large number of databases that are ELECTRONIC WINDOWS into the most intimate details of people's lives. What is even more disturbing is that it is usually impossible to know who is looking in. Thus these databases are like ONE WAY MIRRORS.

Encryption can serve as a curtain. Therefore the need for a civilian (or non-governmental) effort in cryptography is a strong one. Research results have shown that databases used for statistical purposes are subject to compromise. Using harmless-looking queries (questions), such as asking for the AVERAGE income of individuals in certain categories, it is possible to compromise a database.

The use of databases in employment can result in the accumulation of records on individuals containing data that is both performance relevant as well as data that is subject to privacy protection. The only effective methods for maintaining separation of such data involve encryption. (Preventing the collection of data of certain types is not feasible.)

OPERATING SYSTEM SECURITY

Operating systems are computer programs that perform a large number of functions among which are: 1) the management of resources attached to a computer (such as tapes, disks, memory, files, programs, messages, etc.) 2) allowing several users to compute simultaneously on the same computer.

These tasks are very complicated. Insuring that access to resources is proper (from a security viewpoint) is a problem that has not been satisfactorily resolved. Operating systems may have loopholes that may allow a user to gain access to resources that are supposed to be inaccessible.

The importance of encryption in the design of secure operating systems is demonstrated in the recent design proposals for secure systems.

COMMUNICATION SECURITY

This is the most well understood of the sub-areas of information protection. Historically data was most vulnerable when it was transmitted (or communicated) in some way. Until recently this was the main area of application for encryption. This has changed. New problems in protection of data during communication have arisen that greatly affect the average person in day-to-day activities. The emergence of COMPUTER NETWORKS has led to new applications that threaten privacy to a degree that was not possible before. For example, as the credit card operations go "on line", (i.e., gain instant access to a computer that can authorize the charge or service), suddenly, data that was more or less unavailable before is put on communication lines.

New applications, such as Electronic Mail and Electronic Funds Transfer, require the use of encryption. Other applications, such as those in personal computing, will continue to be discovered as computers proliferate.

RESTRAINTS

The ACE PCSG began by considering the recommendation of model legislation for PRIOR RESTRAINT on cryptology papers. The committee's decision to go ahead and recommend restraints (first mandatory and later voluntary) had no basis whatsoever.

The following constitute some of the arguments against restraints:

1. The National Security interests of the country are considerably broader than the narrow mission of the NSA, which in a nutshell is DATA GATHERING.

The PCSG refused to address the question of whether the broad interests of the country (which include such things as Privacy Protection) would outweigh the risks *(if any)* to the NSA's mission. The committee felt that this was too abstract an issue. The importance of Cryptography to telecommunication protection as well as other computer security areas (outlined above), however, is as concrete an issue as one could hope to get. The need for a non-governmental effort in this area is crystal clear in view of the remarkable insensitivity of the common carriers to the public's concern about privacy. The reported foreign intelligence activities in this country against individuals (or corporations) attest to this. As it was pointed out above, the increase in the level of computerization heightens the need for a cryptographic effort independent of the government.

2. Restraints would adversely affect the quality and direction of basic research in computer science, engineering, and mathematics.

The impact of any types of restraints on research (either applied or basic) was not adequately addressed by the committee. The effects of withholding basic or applied research results relating to cryptography would handicap researchers, not only in data security, but in computer science and engineering and allied areas. The restraints would remove from the public domain the most interesting and intellectually stimulating results. The long-term consequences would no doubt be harmful to the Nation.

Consider the problem of implementation of restraints. It has been suggested that the test for whether a paper should be withheld from publication might be "the degree of significant use" of a cryptosystem. A case in point is the use of the Rivest-Shamir-Adleman cryptosystem in the Zero Power Plutonium reactor. The security of this system depends on the fact that no efficient methods for factoring a large number have been found. In view of the recent results related to this problem, some researchers now believe that such methods might indeed be found. If that were to occur, then a solution might have to be suppressed since some can argue that the application just mentioned constitutes a significant use. The solution to an age-old problem would thus be withheld from researchers.

3. Restraints would be unconstitutional.

The constitutionality of restraints was only glossed over. It was pointed out that in one case where legislation did exist (the ITAR) the Justice Department had issued an opinion that that was unconstitutional. It was suggested that the Justice Department opinion on ITAR was in dispute.

4. Restraints, the implementation of which is to include the cooperation of editors of journals, would cause international complications.

The technical societies that publish the journals would have serious problems with having to cooperate with the NSA. They may find themselves subjected to harassment by other governments since many of the societies are international in scope. This would have an effect on the scientific exchanges, treaties, and understandings. (For example, it might affect such things as what journals constitute "intelligence"journals.) It would set precedent for the discussions on the freedom of the press that are conducted elsewhere. There may very well be an impact on the Transborder Data Flow guidelines recently concluded.

Finally, the journals may find it impossible to carry out the implementation of such restraints because their charters would not allow it.

5. Restraints would lead to legal entanglements with existing laws.

Restraints may put the researchers in a very difficult position with respect to the laws that already exist:

a. The impact of restraints on the patent secrecy process is significant. The restraints would enhance the government's ability to issue these orders.

If the restraints were to be put in effect, then an applicant for a patent based on the now unpublished result would risk a secrecy order since existing law disallows the government from issuing a secrecy order when the subject matter had been published in the open literature.

b. Researchers may find themselves violating state statutes if they were to comply with restraints.

The committee did not address the potential impact of restraints on existing laws. Since research in most cases is funded in part by state funds, a researcher may not be able to simply drop some results from his/her paper for nontechnical reasons.

6. Restraints, even if desirable or possible, would be ineffective in achieving the NSA's objectives.

The very nature of Cryptography makes it unlikely that restraints would be effective barriers to TECHNOLOGY TRANSFER. Cryptography is not hardware intensive. The main hardware needed for implementation is a microprocessor, an abundantly available and inexpensive device. This means that the restraints would be placed on an activity that is largely intellectual — design and analysis of algorithms.

Since the hardware involved in the design of cryptosystems is not controlled, the restraints would result in removing from the public domain the most interesting algorithms, thus seriously handicapping the researchers in this country. Researchers in other countries, who are not likely to have such restraints, would be quite capable of designing their own algorithms. THEY WOULD ANYWAY!! The design of cryptosystems involves a large degree of distrust and suspicion about the possibility that a system will have a shortcut known only to the designer. Thus, as David Kahn has said, governments are unlikely to trust anyone but their own scientists and engineers. One can even argue that if in fact they were to use the systems designed in this country, then that would present opportunities for intelligence gathering.

7. The likelihood that basic research results would lead to efficient cryptanalytic attacks against the government's cryptosystems is practically nil.

The NSA claims that the basic or applied research results might lead to efficient attacks against the systems that they have designed. This is not likely because *researchers do not engage in cryptanalysis.*

Cryptanalysis is a tedious and time/resource consuming activity. Inverting a cryptographic function is not that attractive. These mathematical functions are for the most part "ugly" functions that, even if inverted, could be made just as difficult by a change of one or two symbols. Thus the intellectual attraction is not there. Furthermore, researchers do not have access to NSA's cryptosystems. The analogy that Martin Hellman used was that of a chemist inventing a chemical such that a drop would eat through a Sherman tank. The likelihood of such an occurrence is of course high if the tanks were made of plastic. Besides, the very concept of denying the public the opportunity to advance in a field just to enable the NSA to perform its job is alien to the traditions of this country.

REMARKS

While the PCSG has retreated from recommending model legislation, its actions are still troublesome. The very recommendation that restraints be put into effect, even if voluntary, is dangerous. There already is talk of a trial period to see if the NSA is happy about the outcome. There is clear indication that if the NSA is not, then legislation will be sought. At that time, this committee's recommendation could be used as expert testimony that NSA's claims are valid. Such a conclusion would be erroneous. The majority of the committee members are not researchers in data security or cryptography or computer science or engineering.

In conclusion, I find NSA's effort to control cryptography to be unnecessary, divisive, wasteful, and chilling. The NSA can perform its mission the old-fashioned way: STAY AHEAD OF OTHERS.

ACKNOWLEDGMENTS

I would like to thank the following individuals, with whom I have had a number of discussions on this subject:

David Kahn, Carl Hammer, Martin Hellman, Ronald Rivest, Len Adleman, Gutavus Simmons, W. Richards Adrion, Richard Lipton, Richard DeMillo, Whitefield Diffie, Ralph Merkle, David Watters, Charles Wilk and Gerald Sturges.